Richard D. McCune, SBN. 132124
E-mail: rdm@mccunewright.com
David C. Wright, State Bar No. 177468
E-Mail: dcw@mccunewright.com
Michele M. Vercoski, SBN. 244010
E-mail: mmv@mccunewright.com
MCCUNEWRIGHT LLP
2068 Orange Tree Lane, Suite 216
Redlands, California 92374
Telephone: (909) 557-1250
Facsimile: (909) 557-1275

John A. Yanchunis, FL SBN. 324681*
E-mail: jyanchunis@ForThePeople.com
Marcio W. Valladares, FL SBN. 0986917 *
E-mail: mvalladares@forthepeople.com
Patrick A. Barthle, III, FL SBN. 99286*
Email: pbarthle@forthepeople.com
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida, 33602
Telephone: (813) 223-5505
Facsimile: (813) 222-4738

Attorneys for Plaintiff and Putative Classes
[LIST OF ADDITIONAL COUNSEL CONTINUED ON NEXT PAGE]

IN THE UNITED STATES DISTRICT COURT

CENTRAL DISTRICT-EASTERN DIVISION

FRANK VARELA, on behalf of himself and all other similarly situated,

Plaintiff,

v.

LAMPS PLUS, INC., LAMPS PLUS CENTENNIAL, INC., LAMPS PLUS HOLDINGS, INC., and DOES 1 through 10, inclusive,

Defendants.

Case No: 5:16-cv-00577

CLASS ACTION COMPLAINT

1. NEGLIGENCE;
2. BREACH OF IMPLIED CONTRACT;
3. VIOLATION OF CALIFORNIA CONSUMER RECORDS ACT (CAL. CIV. CODE, §§ 1798.81.5, 1798.82);
4. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW (CAL. BUS. & PROF. CODE, § 17200);

5. INVASION OF PRIVACY;

6. NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT.

DEMAND FOR JURY TRIAL

Steven W. Teppler, Florida State Bar No. 14787*
Email: steppler@abbottlawpa.com
ABBOTT LAW GROUP, P.A.
2929 Plummer Cove Road,
Suite 300
Jacksonville, FL 32223
Telephone: (904) 292-1111
Facsimile: (904) 292-1220

Joel R. Rhine, NC State Bar No. 16028*
Email: jrr@rhinelawfirm.com
RHINE LAW FIRM, P.C.
1612 Military Cutoff
Wilmington, NC 28403
Telephone: (910) 772-9960
Facsimile: (910) 772-9062

**Pro Hac Vice* Applications to be submitted
Attorneys for Plaintiffs and Putative Classes

CLASS ACTION COMPLAINT

Plaintiff Frank Varela, individually and on behalf of a class of persons similarly situated (the "Class" or "Class Members"), brings this class action against Defendants, Lamps Plus, Inc., Lamps Plus Centennial, Inc., Lamps Plus Holdings, Inc., and Does 1 through 10 (collectively "Defendants"). The basis for and the relief sought is set forth below.

I. FACTUAL ALLEGATIONS

1. This case arises out of the cyber-breach of Defendants' providing payroll information to unauthorized recipients that compromised the security of sensitive personal information of approximately 1,300 employees (the "Data Breach"). Plaintiff and the Class Members include current and former employees of Defendants, as well as family members and close friends of said employees whose personal information was collected during the employees' hiring, tenure, promotions, demotions, any and all considerations made for any and all reasons, before, during and/or after the employee/employer relationship.

2. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this class action against Defendants for their failure to adequately safeguard and secure personally identifiable information, including names, dates of birth, social security numbers, billing information, wages, state and federal income tax, and other types of information (collectively "Personally Identifiable Information" or "PII") of Plaintiff and Class Members.

3. Defendants are the nation's largest lighting retailer. Lamps Plus is a Los Angeles based, privately held company that maintains multiple e-commerce sites and operates dozens of retail showrooms across the Western United States. Defendants have built their success upon delivering consumers and professional service, selection, quality and style in home lighting and furnishings. Defendants also manufacture, wholesale and distribute thousands of designs. Lamps Plus, Inc. maintains international offices and manufacturing plants, and its website was picked as one of the top fifty retail websites by

Internet Retailer magazine in 2004. The company has made the top 200 of the list every year it has been published. Defendants' family of websites include www.LampsPlus.com; www.55DowningStreet.com; and www.LampsPlusOpenBox.com.

4. The present case stems from the unauthorized access of Defendants' employee information. On or about March 3, 2016, Cindy Beeson, a human resourses representative from Lamps Plus, Inc. stated that "an unknown criminal sent an email to an individual at Lamps Plus, which was intended to look as though it came from another Lamps Plus employee. The response to that email resulted in the criminal obtaining copies of [employees'] W-2 income and tax withholding statement, along with those of every other employee who worked for [Defendants] during 2015."

5. These records included personal details such as name, address and date of birth, as well as Social Security numbers and tax identification numbers and financial information from W-2 income, earnings, and tax-withholding statements, or PII.

6. Following the public announcement of the breach, Defendants acknowledged the importance of the privacy and security of its employees, offering to provide free identity monitoring services for its employees for one year. On March 25, 2016, Lamps Plus Chief Financial Officer Clark Linstone issued a statement on the impact of the data breach on the employees, which read in part: "Unfortunately, Lamps Plus employees during the 2015 calendar year are impacted," and the company is providing "one-year of credit monitoring services, identity counseling and other services."

7. Plaintiff Frank Varela ("Plaintiff" or "Varela") is an employee of Defendant Lamps Plus, Inc., and has been an employee of Lamps Plus, Inc., for approximately nine years. Plaintiff Varela is employed as a Warehouseman at Defendants' warehouse located in Redlands, California, and was a paid employee for the 2015 fiscal year. Based on information and belief, Plaintiff Varela's PII was stolen in the Data Breach.

8. Based on information and belief, Plaintiff Varela's 2015 income taxes were fraudulently filed with the PII stolen in the Data Breach. Plaintiff Varela received a letter

from the IRS dated March 16, 2016, confirming that there was a fraudulent income tax filing under Plaintiff's name. On March 21, 2016, Plaintiff called the IRS and advised them that his identity was stolen in the Data Breach and that he had not filed his tax returns and therefore the filed returns were fraudulent. Plaintiff signed and faxed IRS Form 14039 – Identity Theft Affidavit – to the IRS to formally notify the IRS that Plaintiff's PII was stolen.

9. The IRS then told Plaintiff Varela that he and his wife, Darlene Varela, would be given a special PIN number to include in their paper filing this year and that he would not be able to e-file for the foreseeable future. Plaintiff Varela and his wife are reasonably concerned about his and his wife's future, as their PII was in the stolen tax data from Defendants. The stolen information also includes their names, residential address, dates of birth, telephone numbers, bank account information, social security number, wage and income information, and other personal information. Now their PII lies in the hands of the fraudsters.

10. Prior to the Data Breach, neither Plaintiff Varela nor his wife, Darlene Varela, had ever been the victims of stolen identity or been involved in a data breach. In fact, Darlene Varela has experience working as a mortgage fraud investigator and has also been hyper vigilant and her and her husband's PII and financial information. Plaintiff's wife has always monitored their personal accounts more closely than the average person and is devastated by the Data Breach. She now checks the family's accounts several times a day. She has seen firsthand the massive havoc that stolen PII can wreak on the lives of the victims.

11. Because the Defendants required that Plaintiff Varela provide this highly important personal data to them as a condition of employment and in exchange for a paycheck, Plaintiff Varela had a reasonable expectation that Defendants would have in place reasonable and appropriate security measures to insure that his and his wife's personal data were secure.

12. Plaintiff Varela and/or his wife have spent more than 30 hours dealing with the ramifications of this fraud. They have made phone calls to the IRS, filled out forms, attended meetings, went to their bank in person to notify of fraud and change passwords, and Plaintiff's wife personally monitors all financial accounts several times per day in between working her full time job. Further, because of this fraud, Plaintiff is no longer eligible for electronic filing of his tax returns for the "foreseeable future." Plaintiff reasonably believes that his PII was compromised and obtained by the cybercriminals through the Defendants' systems. Further, because the Defendants permitted fraudsters' access to his account information by its knowing and willful release of said information directly to the fraudsters, Plaintiff is at a heightened risk of further identity theft requiring him to pay indefinitely for on-going credit monitoring. Currently, Plaintiff and his wife are paying twelve dollars per month for credit monitoring. Plaintiff and his wife will continue to monitor their personal accounts for life.

13. Based on information and belief, Plaintiff is not the only one who had a fraudulent income tax filing attempt with his PII; other Class Members also had fraudulent tax returns filed after the Data Breach.

14. What makes this recent breach so ironic is that Defendants released their employees' PII to a third-party criminal without good cause or reasonable diligence. In light of all of the recent and rampant data breaches in the public and private sectors, Defendants knew or should have known to have safeguards in place to maintain and secure their employees' PII.

15. Defendants' security failures enabled the criminals to steal Plaintiff's and the other Class Members' PII from within Defendants' own computer systems and put Plaintiff and the other Class Members' financial information at serious, immediate, and ongoing risk. The practice with such data breaches is that hackers will continue to use the information they obtained as a result of inadequate security, as with Defendants here, to exploit and injure Class Members by selling the PII to third parties and otherwise using

the PII for illicit purposes. Defendants' inadequate security of their employees' PII now blankets Plaintiff and the other Class Members with a known and documented risk.

16. The Data Breach was caused and enabled by Defendants' violation of its obligation to abide by best practices and industry standards concerning the security of its computer and payroll processing systems. Defendants failed to comply with security standards and allowed its employees' PII to be compromised by cutting corners on security measures that could have prevented or mitigated the Data Breach. Defendants' failure to monitor who accessed its networks and Plaintiff's and the other Class Members' PII resulted in unauthorized individuals gaining access to its networks by simply posing as a Lamps Plus employee.

17. Defendants also failed to timely disclose the extent of the Data Breach, failed to individually notify each of the affected individuals of the Data Breach in a timely manner, and failed to take other reasonable steps to clearly and conspicuously inform Plaintiff and the other Class Members of the nature and extent of the Data Breach. By failing to provide adequate notice, Defendants prevented Plaintiffs from protecting themselves from the consequences of the Data Breach. Many affected employees first learned that their PII had been stolen only after being notified of fraudulent activity when some employees attempted to file their 2015 tax returns and the IRS advised them that tax returns had already been filed in their name.

18. As a result of Defendants' failure to adequately protect and secure Class Members' PII, some yet unidentified individual or individuals gained access to and obtained PII belonging to Class Members in disregard for the privacy and security rights of Plaintiff and Class Members and for the obvious purpose of using this information for personal gain to the damage and detriment of Plaintiff and Class Members.

19. The ramifications of Defendants' failure to keep Class Members' PII secure are severe and can result in the theft of the identity of a large number of people. Identity theft occurs when someone uses another's PII, such as the person's name, address, and Social Security numbers to commit fraud or other crimes. The Federal Trade

Commission ("FTC") estimates that as many as 9 million Americans have their identities stolen each year.

20. Social security information of the type that was wrongfully accessed is entitled to high level of protection due to its private and confidential nature. The protection to which this information is entitled is recognized by statutory and case law.

21. The combination of this information with the names, addresses and Social Security numbers of Class Members enhances the sensitivity of this information, making it susceptible to abuse and exploitation. Defendants knew and understood the confidential and private nature of the PII of Class Members and owed a duty to Class Members to protect and maintain the confidentiality and security of their PII.

22. In particular, social security numbers are a form of national identifier and are not easily replaced. The FTC warns consumers to protect their social security numbers, and to give out the number only if absolutely necessary. *See* www.ftc.gov/idtheft. Similarly, the Social Security Administration warns consumers to safeguard their social security numbers and to be careful about sharing those numbers. *See* http://www.ssa.gov/pubs/EN-05-10064.pdf.

23. It is well known, and the subject of many media reports, that PII data is highly coveted by, and a frequent target of thieves. The criminal underground recognizes the value in PII and is willing to pay hackers to go get it. PII data has been stolen and sold by the criminal underground on many occasions in the past, a fact well publicized in the public press.

24. Criminals are increasingly after PII because they can use biographical data from multiple sources to perpetuate more and larger thefts. Illicitly obtained PII, sometimes aggregated from different breaches, is sold on the black market, including on websites, as a product at a set price.

25. Identity thieves can use identifying data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit or credit cards.

26. Identity thieves can use personal information to perpetuate a variety of crimes that harm the victims. For instance, identity thieves (a) may commit various types of government crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture; (b) may use the victim's information to obtain government benefits; or (c) may file fraudulent tax returns using the victim's information to obtain a fraudulent refund. The IRS identified more than 2.9 million incidents of identity theft in 2013, and the IRS has described identity theft as the number one scam for 2014. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

27. It is well known and the subject of many media reports that PII data is highly coveted by and a frequent target of hackers and is often easily taken because it is inadequately protected. Legitimate organizations and the criminal underground alike recognize the value in PII. Otherwise, they would not pay for it or aggressively seek it. PII data has been stolen and sold by the criminal underground on many occasions in the past, including PII held by many large corporations in prior data breaches, and accounts of the thefts and unauthorized access have been the subject of many media reports. While Payment Card Industry data (PCI) is more regulated and protected then PII, criminals are increasingly after PII because they can use biographical data from multiple sources to perpetuate more and larger thefts. *See* Verizon 2014 PCI Compliance Report, available at http://www.verizonenterprise.com/resources/reports/rp_pci-report-2014_en_xg.pdf (hereafter "Verizon Report"). Illicitly obtained PII and PCI, sometimes aggregated from different breaches, is sold on the black market, including on websites, as a product at a set price. *See, e.g.*, KREBS ON SECURITY, *How Much is Your Identity Worth*, http://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth/ (last visited October 5, 2015). Despite all of the publically available knowledge of the continued compromises of PII, Defendants' approach to maintaining the privacy of

Plaintiff's and Class Members' PII was lackadaisical, cavalier, and reckless; at the very least it was negligent.

28. The ramifications of Defendants' failure to keep Class Members' PII secure are severe. Once PII is stolen, fraudulent use of that information and the damage to their employees may continue for years.

29. Annual monetary losses from identity theft are in the billions of dollars. According to publish reports, those losses were $21 billion in 2013.

30. As a result of Defendants' failure to prevent the breach, Plaintiff and Class Members have suffered and will continue to suffer damages, including pecuniary losses, anxiety, and emotional distress. They have suffered or are at increased risk of suffering from:

- the loss of the opportunity to control how their PII is used;
- the diminution in the value and/or use of their PII, entrusted to Defendants for the purpose of obtaining cellular telephone services with the understanding that Defendants and its employees/managers would safeguard their PII against theft and not allow access and misuse of their PII by others;
- the compromise, publication and/or theft of their PII;
- out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts;
- lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse;
- costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets;

- unauthorized use of compromised PII to open new financial and/or health care or medical accounts;
- the continued risk to their PII, which remains in the Defendants possession and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the PII in their possession;
- current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the data breach for the remainder of the lives of the Class Members and their families/spouses/dependents.

31. Accordingly, Plaintiff, individually and on behalf of other Members of the Class, assert claims for breach of implied contract, negligence, invasion of privacy, and seek injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief authorized in equity or by law.

II. PARTIES, JURISDICTION AND VENUE

32. Plaintiff, Frank Varela, is a resident of the state of California, and resided in that state at all times herein material.

33. Lamps Plus, Inc., is a California corporation with its principal offices located at 20250 Plummer Street, Chatsworth, California 91311.

34. Lamps Plus – Centennial, Inc., is a California corporation with its principal offices located at 20250 Plummer Street, Chatsworth, California 91311.

35. Lamps Plus Holding, Inc., is a California corporation with its principal offices located at 20250 Plummer Street, Chatsworth, California 91311.

36. The true names capacities of Defendants sued herein as DOES 1 through 10, inclusive, are currently unknown to Plaintiff, who therefore sues such Defendants by such fictitious names. Each of the Defendants designated herein as DOE is legally responsible in some manner for the unlawful acts referred to herein. Plaintiff will seek leave of Court to amend this Complaint to reflect the true names and capacities of the Defendants designated herein as DOES if and when their identities become known.

37. Based on information and belief, Plaintiff alleges that at all times mentioned herein, each and every Defendant was acting as an agent and/or employee of each of the other Defendants, and at all times mentioned was acting within the course and scope of said agency and/or employment with full knowledge, permission, and consent of each of the other Defendants. In addition, each of the acts and/or omissions of each Defendant alleged herein were made known to, and ratified by, each of the other Defendants.

38. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs; there are more than 100 putative Class Members defined below.

39. Court has federal question jurisdiction under 28 U.S.C. § 1331 in light of the Fair Credit Reporting Act alleged below; supplemental jurisdiction over state claims exists under 28 U.S.C. § 1367.

III. CLASS ACTION ALLEGATIONS

40. Plaintiff brings this action pursuant to Rule 23 (a), (b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure. He brings this action on his own behalf and on behalf of all other similarly situated persons. Plaintiff is informed and believes there are thousands of Members in the proposed Class. The proposed Class consists of:

> **All persons throughout the United States who were employees, independent contractors, or otherwise paid by Lamps Plus, Inc., Lamps Plus – Centennial, Inc., or Lamps Plus Holdings, Inc., during the 2015 calendar year.**

41. To be excluded from the Class are all officers and directors of Defendants and the Judges assigned to and who may preside over this case and the Judges' staff.

42. ***Numerosity.*** The Class is so numerous that joinder of all Members is impracticable. Upon information and belief, there are at least over one thousand individuals whose PII has been stolen from Defendants. These individuals are identifiable from Plaintiff's description of the Class, and from Defendants' records, and/or from the records of third parties accessible through discovery.

43. ***Typicality.*** Plaintiff's claims are typical of those of other Class Members, as there are no material differences in the facts and law underlying their claims and Plaintiff's prosecution of their claims will advance the claims of all Class Members. By aggressively pursuing his own claim, the Plaintiff will necessarily be concurrently aggressively pursuing the claims of Class Members.

44. ***Adequacy.*** Plaintiff will fairly and adequately protect the interests of the Class and is willing to submit to the Court such evidence as the Court may deem necessary to ensure that the interests of the Class are properly served. Plaintiff has retained competent counsel experienced in the prosecution of this type of Class litigation.

45. ***Common Questions and Predominate.*** There are numerous and substantial questions of law or fact common to all Members of the Class that will predominate over any individual issues, including but not limited to:

a. Whether Defendants negligently failed to implement and maintain commercially reasonable procedures to ensure the security of Class Members' PII;

b. Whether Defendants, after discovering the data breach, negligently failed to take steps to: (i) promptly notify the Class; and (ii) protect Class Members in a timely manner;

c. Whether Defendants owed a fiduciary obligation to the Members of the Class and whether that fiduciary obligation was breached as a result of the Defendants' actions and inactions;

d. Whether there exists an implied contract between the Members of the Class on one hand, and Defendants on the other hand, and whether the actions and inactions of Defendants breached that implied contract;

e. Whether Defendants should be required to pay for the reasonable cost of credit monitoring services; and

f. To the extent that some Class Members have already sustained damage as a result of identity theft brought about by Defendants' actions and inactions, what is the proper measure of damages, and the proper method for determining those damages, on a Class-wide basis.

46. ***Superiority.*** Class treatment of the claims set forth in this Complaint is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it

impracticable or impossible for the proposed Class Members to prosecute their claims individually. Absent a class action, a multiplicity of individual lawsuits would be required to address the claims between Class Members and Defendants so that inconsistent treatment and adjudication of the claims would likely result.

47. The litigation of Plaintiff's claims is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

48. Adequate notice can be given to Class Members directly using information maintained in Defendants' records and/or through publication.

49. Unless a Class-wide injunction is issued, Defendants may continue in its failure to properly secure the PII of Class Members; Defendants may continue to refuse to provide proper notification to Class Members regarding the scope of the data breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

50. Defendants have acted, or refused to act, on grounds that apply generally to the Class, making final injunctive and declaratory relief appropriate to the Class as a whole. Defendants' acts and omissions are the direct and proximate cause of damage described more fully elsewhere in this Complaint.

FIRST CAUSE OF ACTION

Negligence

51. Plaintiff and the Class incorporate by reference each preceding paragraph as though fully set forth at length herein.

52. Upon accepting and storing Class Members' PII in its respective computer database systems, Defendants undertook and owed a duty to Class Members to exercise reasonable care. It was Defendants' obligation to secure and safeguard that information and to utilize commercially reasonable methods to do so. Defendants knew that the PII was private and confidential and should be protected as private and confidential.

53. Defendants breached its duties to Class Members to adequately protect and safeguard this information by knowingly disregarding standard principles relating to the securing of PII. Defendants negligently failed to provide adequate supervision and oversight of the PII which was, and is, entrusted to them, in spite of the known risks and foreseeable likelihood of breach and misuse. Defendants' failures permitted third persons to gather Class Members' PII, misuse the PII, and intentionally disclose it to others without consent.

54. The law also imposes an affirmative duty on Defendants to timely disclose the theft of the PII so that Class Members could be vigilant in attempting to determine if any of their accounts or assets had been stolen through identity theft.

55. Through Defendants' acts and omissions described in this Complaint, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Class Members' PII during the time it was within Defendants' possession or control.

56. Further, through their failure to provide timely and clear notification of the data breach to employees, Defendants negligently prevented Class Members from taking meaningful, proactive steps to investigate possible identity theft.

57. Defendants improperly and inadequately safeguarded PII of Class Members in deviation of standard industry rules, regulations and practices at the time of the access by unauthorized persons.

58. Given the extensive publicity about the efforts of criminal enterprises to obtain PII, it was foreseeable to Defendants that the Plaintiff's PII in their possession might be attractive to hackers and other criminals.

59. For all the reasons stated above, Defendants' conduct was negligent and departed from reasonable standards of care including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Class Members' PII;

and failing to provide Class Members with timely and sufficient notice that their sensitive PII had been compromised.

60. Neither Plaintiff nor the other Class Members contributed to the data breach or subsequent misuse of their PII as described in this Complaint.

61. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and every member of the Class has been put at risk of identity theft and has an obligation to mitigate damages through credit monitoring services. Defendants are liable to each and every member of the Class for the reasonable costs of future credit monitoring services. Defendants are also liable to those Class Members who have directly sustained damages as a result of their identity theft.

SECOND CAUSE OF ACTION

Breach of Implied Contract

62. Plaintiff and the Class incorporate by reference each preceding paragraph as though fully set forth at length herein.

63. When the Plaintiff became an employee of Defendants, a contract was created between the Plaintiff and Defendants. The same is true with respect to the contractual relationship that arose between Defendants and every other member of the Class.

64. Defendants agreed to provide employees with a paycheck in exchange for their services.

65. Implicit in the agreement made by Defendants was an understanding that, as part of employment, Defendants would protect the sensitive information provided by the Class, as required by accepted standards in Defendants' businesses and in compliance with federal and state employment and income tax laws.

66. Defendants breached its implied agreement causing damages to the members of the Class for which recovery should be made as demanded hereafter.

THIRD CAUSE OF ACTION

Violation of California's Consumer Records Act

(Cal. Civ. Code § 1798.80, *et seq.*)

67. Plaintiff and the Class incorporate by reference each preceding paragraph as though fully set forth at length herein.

68. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Civil Code section 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

69. Defendants are a "business" within the meaning of Civil Code section 1798.80(a).

70. Plaintiff and Members of the Class are "individual[s]" within the meaning of Civil Code section 1798.80(d).

71. Pursuant to Civil Code sections 1798.80(e) and 1798.81.5(d)(1)(C), the data theft included the theft of "personal information" as meant by those sections, including names, addresses, Social Security numbers, and driver's license or state identification card numbers.

72. The breach of personal data of thousands of former or current employees of Defendants constituted a "breach of the security system" of Defendants, under Civil Code section 1798.82(g).

73. By failing to implement reasonable measures to protect its former and current employees' personal data, Defendants violated Civil Code section 1798.81.5.

74. In addition, by failing to promptly notify all affected former and current and prospective customers of Defendants that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the data breach, Defendants violated Civil Code section 1798.82 of the same title. Defendants'

failure to timely notify employees of the beach has caused Class Members damages because they had to take measures to remediate the breach caused by Defendants' negligence.

75. By violating Civil Code sections 1798.81.5 and 1798.82, Defendants "may be enjoined" under Civil Code section 1798.84(e).

76. Accordingly, Plaintiff and the Class request that the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures to protect employees' data in compliance with the California Customer Records Act, including, but not limited to: (1) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (2) ordering that Defendants engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures; (4) ordering that Defendants purge, delete, and destroy in a reasonable secure manner patient data not necessary for their business operations; (5) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning, real-time network traffic analysis, and security checks; (6) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (7) ordering Defendants to meaningfully educate their former and current and prospective employees about the threats they face as a result of the loss of their personal information to third parties, as well as the steps they must take to protect themselves; and (8) ordering Defendants to implement a written policy for implementation of the items (1) through (7), above.

77. Plaintiff further requests that the Court require Defendants to (1) identify and notify all Members of the Class who have not yet been informed of the data breach;

and (2) to notify affected former and current employees of any future data breaches by email within 24 hours of Defendants' discovery of a breach or possible breach.

78. As a result of Defendants' violation of Civil Code sections 1798.81.5 and 1798.82, Plaintiff, individually and on behalf of the Members of the Class, seeks remedies under Civil Code section 1798.84, specifically, equitable relief.

79. Plaintiff, individually and on behalf of the Members of the Class, also seeks reasonable attorney's fees and costs under applicable law, including Code of Civil Procedure section 1021.5.

FOURTH CAUSE OF ACTION

Violation of California Unfair Competition Laws

(Bus. & Prof. Code, § 17200)

80. Plaintiff and the Class incorporate by reference each preceding paragraph as though fully set forth at length herein.

81. Plaintiff brings this cause of action on behalf of Plaintiff and the Class Members whose personal information was compromised as a result of the data breach.

82. Defendants' acts and practices, as alleged in this complaint, constitute unlawful and unfair business practices in violation of the Unfair Competition Law ("UCL"), Bus. & Prof. Code, § 17200, *et seq.*

83. Defendants' acts and practices, as alleged in this complaint, constitute unlawful and unfair practices in that they violate Civil Code section 1798.80, *et seq.*, and because Defendants' conduct was negligent.

84. Defendants' practices were unlawful and in violation of Civil Code section 1798.81.5(b) because Defendants failed to take reasonable security measures in protecting their former and current and prospective employees' personal data.

85. Defendants' practices were also unlawful and in violation of Civil Code section 1798.82 because Defendants unreasonably delayed informing Plaintiff and Members of the Class about the breach of security after Defendants knew that the data breach occurred.

86. The acts, omissions, and conduct of Defendants constitute a violation of the unlawful prong of the UCL because they failed to comport with a reasonable standard of care and public policy as reflected in statutes such as the Information Practices Act of 1977, Civ. Code, § 1798, *et seq.*, and the California Customer Records Act, Civ. Code, § 1798.80, *et seq.*, which seek to protect individuals' data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

87. Defendants violated the "unfair" prong of the UCL because their acts and/or omissions were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class Members, and because their acts and/or omissions constitute conduct that undermines or violates the stated policies underlying the California Customer Records Act and other privacy statutes. In enacting the California Customer Records Act, the Legislature state that: "[i]dentity theft is costly to the marketplace and to consumers" and that "victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative." (2002 Cal. Legis. Serv. Ch. 1054 (A.B. 700) (WEST).) Defendants' conduct also undermines California public policy as reflected in other statutes such as the Information Practices Act of 1977, Civ. Code, § 1798, *et seq.*, which seeks to protect individuals' data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

88. As a direct and proximate result of Defendants' unlawful business practices as alleged herein, Plaintiff and Members of the Class have suffered the following injuries in fact and losses of money or property: (1) loss of opportunity to control how their PII is used; (2) diminution in the value and/or use of their PII; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft or unauthorized use of financial and medical costs; (5) lost opportunity costs and loss of productivity from efforts to mitigate the actual and future consequences of the theft of PII; (6) cost associated with the inability to use credit and assets frozen or flagged as a result of credit misuse; (7) unauthorized use of

compromised PII; (8) tax fraud or other unauthorized charges to financial, health care, or medical accounts; (9) continued risk to PII that remain in the possession of Defendants, as long as Defendants fail to undertake adequate measures to protect PII; and (10) future costs in terms of time, effort, and money that will be expended to prevent and repair the impact of the data breach.

89. As a direct and proximate result of Defendants' unlawful business practices as alleged herein, Plaintiff and the Class Members face an increased risk of identity theft based on the theft and disclosure of their personal information.

90. As a result of Defendants' violations, Plaintiff and Members of the Class are entitled to injunctive relief, including, but not limited to: (1) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (2) ordering that Defendants engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures; (4) ordering that Defendants purge, delete, and destroy in a reasonable secure manner employee data not necessary for their business operations; (5) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning, real-time network traffic analysis, and securing checks; (6) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal human resources and security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (7) ordering Defendants to meaningfully educate their former and current employees about the threats they face as a result of the loss of their personal information to third parties, as well as the steps they must take to protect themselves; and (8) ordering Defendants to implement a written policy for implementation of the items (1) through (7), above.

91. Because of Defendants' unfair and unlawful business practices, Plaintiff and the Class are entitled to relief, including (1) restitution to Plaintiff and Class Members of the losses they incurred as a result of the data breach; (2) attorneys' fees and costs; (3) declaratory relief; and (4) a permanent injunction enjoining Defendants from their unlawful and unfair practices.

FIFTH CAUSE OF ACTION

Invasion of Privacy

92. Plaintiff and the Class incorporate by reference each preceding paragraph as though fully set forth at length herein.

93. Defendants invaded Plaintiff's and the Class Members' right to privacy by allowing the unauthorized access to Plaintiff's and Class Members' PII and by negligently maintaining the confidentiality of Plaintiff's and Class Members' PII, as set forth above.

94. The intrusion was offensive and objectionable to Plaintiff, the Class Members, and to a reasonable person of ordinary sensibilities in that Plaintiff's and Class Members' PII was disclosed without prior written authorization of Plaintiff and the Class.

95. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff's and the Class Members' provided and disclosed their PII to Defendants, as employees of Lamps Plus, privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class Members were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

96. As a proximate result of Defendants' above action and inaction, Plaintiff's and the Class Members' PII was viewed, printed, distributed, and used by persons without prior written authorization and Plaintiff and the Class Members suffered damages.

97. Defendants are guilty of oppression, fraud, malice, or reckless disregard by permitting the unauthorized disclosure of Plaintiff's and the Class Members' personal

information with a willful and conscious disregard of Plaintiff's and the Class Members' right to privacy.

98. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause Plaintiff and the Class Members great and irreparable injury in that the PII maintained by Defendants can be viewed, printed, distributed, and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff and the Class.

SEVENTH CAUSE OF ACTION

Negligent Violation of the Fair Credit Reporting Act

99. Plaintiff and the Class incorporate by reference each preceding and succeeding paragraph as though fully set forth at length herein.

100. Defendants owed a duty to Plaintiff and Class Members to safeguard the security of their personal employment account information and to adopt and maintain reasonable procedures pursuant to the Fair Credit Reporting Act, 15 U.S.C. § 1681(b) ("FCRA"), including procedures to adequately secure its servers and sufficiently encrypt its passwords, in a manner fair and equitable to employees/consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information.

101. Defendants negligently failed to adopt and maintain reasonable procedures in a manner fair and equitable to employees while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information in compliance with FCRA. In addition, Defendants negligently violated FCRA because, by its failure to maintain reasonable procedures, hackers gained unauthorized access to employee tax/consumer report information absent a permissible purpose.

102. Plaintiff and Class Members suffered actual damages as a result of Defendants' negligent violation of FCRA including but not limited to the lost monetary value of their PII, expenses for credit monitoring and identity theft insurance, out-of-

pocket expenses, anxiety and emotional distress and loss of privacy.

103. Plaintiff and Class Members are entitled to compensation for their actual damages as described above, and attorneys' fees and costs, pursuant to 15 U.S.C. § 1681o(a).

RELIEF SOUGHT

Plaintiff respectfully requests the Court enter a judgment and order as follows:

A. For an order certifying that the action may be maintained as a class action under Rule 23(a), (b(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure; certifying Plaintiff as a representative of the Class defined above and designating his undersigned counsel as counsel for the Class;

B. A mandatory injunction directing that Defendants hereafter adequately safeguard the PII of the Class by implementing improved security procedures and measures;

C. A mandatory injunction requiring that Defendants provide notice to each member of the Class relating to the full nature and extent of their PII that has been accessed by unauthorized persons;

D. For damages as provided by state and federal law;

E. For an award of attorneys' fees and costs as may be permitted by law; and

F. For all other legal and equitable relief as the Court may deem just and proper.

Dated: March 29, 2016

Respectfully submitted,
MCCUNEWRIGHT LLP

By: */s/ Richard D. McCune*
Richard D. McCune
Attorneys for Plaintiffs and Putative Classes

JURY DEMAND

Plaintiffs, on behalf of themselves and the putative Classes, demand a trial by jury on all issues so triable.

Dated: March 29, 2016

MCCUNEWRIGHT LLP

By: */s/ Richard D. McCune*
Richard D. McCune
Attorneys for Plaintiffs and Putative Classes